

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-106552

(43)Date of publication of application : 11.04.2000

(51)Int.Cl.

H04L 9/32
G06F 15/00

(21)Application number : 10-274551

(71)Applicant : HITACHI LTD

(22)Date of filing : 29.09.1998

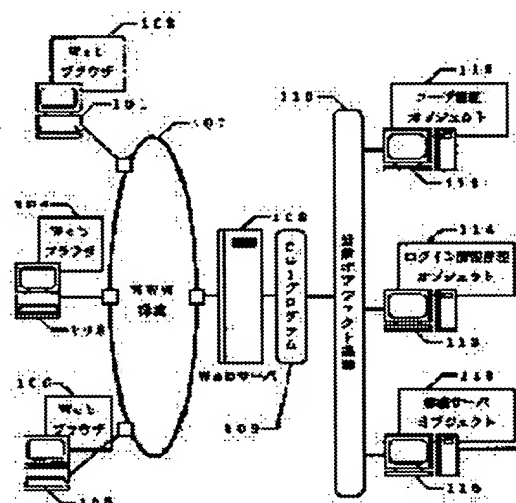
(72)Inventor : ITAYA TAKASHI
HAYASHI SHIGETOSHI
UCHIDA MINORU
KOTAKI NORIYASU
UCHIDA TAKAKO

(54) AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an authentication method that realizes single-sign-on by managing sessions that have already been authenticated in a client-server system where business server objects requiring user authentication are distributed to a network using a distribution object infrastructure and a client uses a communication protocol not managing a connection state such as an HTTP to utilize a business server object.

SOLUTION: A user authentication object 112 makes authentication based on user information received from client computers 101, 103, 105 and a log-in information management object 114 stores sets of information such as user information and user attribute obtained at authentication together with identification information of a session in the case that the authentication is successful to realize single-sign-on in this authentication system.



LEGAL STATUS

[Date of request for examination] 20.09.2001

[Date of sending the examiner's decision of rejection] 14.12.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

THIS PAGE BLANK (USPTO)

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-106552

(P2000-106552A)

(43)公開日 平成12年4月11日(2000.4.11)

| (51)Int.Cl. ⁷ | 識別記号 | F I | テマコード [*] (参考) |
|--------------------------|-------|---------------|-------------------------|
| H 0 4 L 9/32 | | H 0 4 L 9/00 | 6 7 3 D 5 B 0 8 5 |
| G 0 6 F 15/00 | 3 1 0 | G 0 6 F 15/00 | 3 1 0 D 5 J 1 0 4 |
| | 3 3 0 | | 3 3 0 B |
| | | H 0 4 L 9/00 | 6 7 3 A |

審査請求 未請求 請求項の数4 O L (全 6 頁)

(21)出願番号 特願平10-274551

(22)出願日 平成10年9月29日(1998.9.29)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 板谷 孝

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

(72)発明者 林 重年

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

(74)代理人 100068504

弁理士 小川 勝男

最終頁に続く

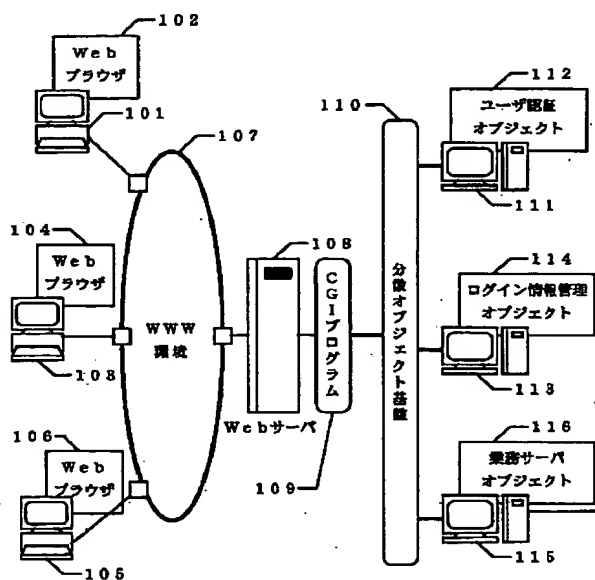
(54)【発明の名称】 認証方法

(57)【要約】

【課題】 ユーザ認証が必要な業務サーバオブジェクトが分散オブジェクト基盤を利用するネットワークに分散しており、クライアントからHTTPのような接続状態を管理しない通信プロトコルを使って業務サーバオブジェクトを利用するクライアント・サーバシステムには、セッションの識別情報を持ち回る必要があるが、ユーザ情報を含む証書をクライアント・サーバの間、サーバ・サーバの間でやりとりすることは、セキュリティ上好ましくない。

【解決手段】 クライアント計算機101、103、105からの受け取ったユーザ情報をもとにユーザ認証オブジェクト112で認証をおこない、認証に成功した場合にセッションの識別情報とともにユーザ情報や認証時に得られるユーザ属性等の情報の組みをログイン情報管理オブジェクト114で保持することにより、シングルサインオンを実現する認証方式。

図1



【特許請求の範囲】

【請求項1】 ユーザ認証が必要な業務サーバオブジェクトが分散オブジェクト基盤を利用するネットワークに分散しており、クライアントからサーバオブジェクトへアクセスするクライアント・サーバシステムにおける認証方法において、

クライアントがサーバにログインするときユーザを識別するユーザ情報書と、セッションを識別するセッション識別子を、ユーザ認証オブジェクトへ送付し、認証された場合、ユーザ認証オブジェクトが当該セッション識別子とユーザ情報をログイン情報管理オブジェクトに登録し保持することを特徴とする認証方法。

【請求項2】 請求項1の認証方法において、クライアントがサーバにログインするときクライアントが認証済みであるかどうかを、ユーザ認証オブジェクトが当該セッション識別子を使ってログイン情報管理オブジェクトに確認することを特徴とする認証方法。

【請求項3】 請求項1の認証方法において、クライアントから業務サーバオブジェクトを呼出す場合、業務サーバオブジェクトは当該セッションが認証済みであるかどうかを、クライアントから受け取ったセッション識別子を使ってログイン情報管理オブジェクトに確認することを特徴とする認証方法。

【請求項4】 請求項1の認証方法において、業務サーバオブジェクトが当該セッションのユーザ情報を必要とする場合に、業務サーバオブジェクトは当該セッションが認証済みであるかどうかをクライアントから受け取ったセッション識別子を使ってログイン情報管理オブジェクトに確認し、業務サーバオブジェクトはログイン情報管理オブジェクトから当該セッションのユーザ情報を取得することを特徴とする認証方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、ユーザ認証が必要な各業務サーバオブジェクトが分散オブジェクト基盤を利用するネットワークに分散しており、クライアントからHTTP（Hypertext Transfer Protocol）のような接続状態を管理しない通信プロトコルを使って業務サーバオブジェクトを利用するクライアント・サーバシステムにおける認証方式に係わり、特に認証済みのセッションを一元管理することで、ネットワークに分散する業務サーバオブジェクトへのシングルサインオンを実現する認証方法に係わる。

【0002】

【従来の技術】 特開平8-292929によれば、遠隔ユーザが入力したユーザ情報がセキュリティ機構で認証された場合、ユーザを識別する働きをするトークンをセキュリティ機構が発行し、ユーザとアプリケーションサーバの間で接続を行うために、接続要求に関連するトークンがセキュリティ機構から発行されたことが確認され

た場合に、ユーザはアプリケーションサーバに接続することが開示されている。

【0003】

【発明が解決しようとする課題】 WWWのような接続状態を管理しないプロトコルを使ったネットワーク環境と分散オブジェクト基盤を組合わせたクライアント・サーバシステムでは、WWW環境でのクライアントとサーバの間だけではなく、分散オブジェクト基盤上の業務サーバオブジェクトの間でも認証が必要となる。このWWW分散オブジェクトを組合わせたクライアント・サーバシステムに、上記の従来の証書を使った認証方式を適用する場合、ユーザ情報を含む証書をセッション識別子の代わりにクライアントサーバの間、サーバサーバの間で持ち回り、しかも一つのセッションの間で、クライアントからの要求の度に証書をサーバとやり取りする必要がある、セキュリティを考えると好ましくない。さらに、その拡張容易性から分散オブジェクト基盤上に多くの業務サーバオブジェクトを配置し、サーバサーバの間で証書をやりとりする頻度が増大する場合、上記セキュリティの問題が大きくなると同時に証書の有効性検証に要する時間も増大する。

【0004】 セッション識別子については、同一ユーザでもセッション毎に異なりユーザ情報を含まないセッション識別子を使うことで、システム外部からの脅威に対して上記セキュリティ上の問題を小さくすることができる。

【0005】 本発明の目的は、ユーザ認証が必要な業務サーバオブジェクトが分散オブジェクト基盤を利用するネットワークに分散しており、クライアントからHTTPのような接続状態を管理しない通信プロトコルを使って業務サーバオブジェクトを利用するクライアント・サーバシステムにおいて、認証済みのセッションを管理することでシングルサインオンを実現する認証方式を提供することにある。

【0006】

【課題を解決するための手段】 本発明は、ユーザ認証が必要な業務サーバオブジェクトが分散オブジェクト基盤を利用するネットワークに分散しており、クライアントからHTTPのような接続状態を管理しない通信プロトコルを使って業務サーバオブジェクトを利用するクライアント・サーバシステムにおいて、シングルサインオンを実現するための認証方式であって、クライアントがサーバにログインする場合、クライアントは、ユーザIDやパスワードなどのユーザ情報もしくはこれらユーザ情報を含む証明書と、当該セッションを識別するためのセッション識別子を、ユーザ認証オブジェクトに渡して認証を行い、認証に成功した場合、ユーザ認証オブジェクトが当該セッション識別子とユーザ情報（ユーザID等）とそのユーザ属性（所属グループ等）をログイン情報管理オブジェクトに登録し保持することを特徴とする

認証方式。

【0007】また上記ユーザ認証オブジェクトでの認証において、認証を要求してきたクライアントが認証済みであるかどうかを、ユーザ認証オブジェクトが当該セッション識別子を使ってログイン情報管理オブジェクトに確認することを特徴とする認証方式。

【0008】さらにクライアントからの業務サーバオブジェクト呼出す場合、業務サーバオブジェクトは、当該セッションが認証済みであるかどうかをクライアントから受け取ったセッション識別子を使ってログイン情報管理オブジェクトに確認することを特徴とする認証方式。

【0009】また業務サーバオブジェクトが当該セッションのユーザ情報を必要とする場合に、業務サーバオブジェクトは当該セッションが認証済みであるかどうかをクライアントから受け取ったセッション識別子を使ってログイン情報管理オブジェクトに確認し、業務サーバオブジェクトはログイン情報管理オブジェクトから当該セッションのユーザ情報やそのユーザ属性を取得することを特徴とする認証方式。

【0010】

【発明の実施の形態】以下、本発明の一実施例について説明する。

【0011】図1はWWW環境と分散オブジェクト環境を組み合わせたクライアント・サーバシステム全体の構成図である。システムはWebブラウザ102、104、106が実行可能なクライアント計算機101、103、105とWebサーバ計算機108によって構成されるWWW環境107と、Webサーバ計算機108内で実行されるCGIプログラム109と、分散オブジェクト基盤110と、ユーザ認証オブジェクト112が実行されるオブジェクトサーバ計算機111とログイン情報管理オブジェクト114が実行されるオブジェクトサーバ113計算機と業務サーバオブジェクト116が実行されるオブジェクトサーバ計算機115によって構成される。図中ではユーザ認証オブジェクト112とログイン情報管理オブジェクト114は異なるオブジェクトサーバ計算機上にあるが同一オブジェクトサーバ計算機上にある場合もある。同様に業務サーバオブジェクト116も同一オブジェクトサーバ計算機に複数あってもよい。これらの物理的配置の制限は分散オブジェクト基盤110によって決められるものである。

【0012】図2以降はクライアント計算機101、102、103でのユーザのログインから認証および業務サーバオブジェクト116を実行するまでの流れ図である。図面の大きさの都合上、複数のフェーズに分けて説明する。

【0013】図2はログイン情報管理オブジェクト114の認証済みのセッション識別子（以下「SID」と略す。）および対応するユーザ情報等のUIDの管理方式の一例である。ここではユーザ情報としてユーザID

（以下「UID」と略す。）および他のユーザ属性を管理しているが、SID以外の情報の種類数はシステムに応じて変わる。本例では表形式での管理方式でありセッション管理テーブル201はSID、UID、必要であればユーザ属性を管理するもので単純な表形式のデータ構造で十分対応可能である。

【0014】図3はユーザが目的とするアプリケーションを実行するためにWebブラウザ102などからWebサーバ計算機108へアクセスしログイン画面が表示されるまでの流れである。ユーザがWebブラウザ102上でログイン画面のURL（Uniform Resource Locator）を入力（ステップ301）する。URLが入力されるとWebブラウザ102はURLに記述されたWebサーバ計算機108へHTTPによりアクセスする。アクセスされたWebサーバ計算機108はCGIプログラム109を起動する（ステップ302）。CGIプログラム109はSIDを生成し（ステップ303）、このSIDをCookieに設定し（ステップ304）、ログイン画面を表示するためのHTML（Hyper Text Markup Language）を生成し（ステップ305）、生成したHTMLとCookieをWebブラウザ102に返す。Webブラウザ102は受け取ったHTMLを表示することでログイン画面を表示する（ステップ306）。

【0015】図4はWebブラウザ102上に表示されたログイン画面からユーザがユーザIDとパスワード（以下「PWD」と略す。）を入力し、ユーザ認証オブジェクト112で認証処理が行われログイン情報管理オブジェクト114にSIDとUIDとユーザ属性が登録されるまでの流れ図である。なお、図4以降Webサーバ計算機108はWebブラウザ102とCGIプログラム109間を、分散オブジェクト基盤110はCGIプログラム109とオブジェクト間を仲介する以外の処理はなく、本発明での重要な部分にはならないので説明および図から省略する。

【0016】Webブラウザ102に表示されたログイン画面でユーザがUIDとPWDを入力する（ステップ401）。入力されたUID、PWDとCookieに設定されたSIDがCGIプログラムに渡る。CGIプログラムは分散オブジェクト基盤110上にあるユーザ認証オブジェクト112に対しUID、PWD、SIDを渡しログイン処理を依頼する（ステップ402）。ユーザ認証オブジェクト112はまずログイン情報管理オブジェクト114に渡されたSIDを使って認証済みかどうかの検証を依頼する（ステップ403）。ログイン情報管理オブジェクト114ではセッション管理テーブル201内を検索（ステップ404）し渡されたSIDが登録済みかどうかの結果をユーザ認証オブジェクト112に返す。同一UIDでの複数ログインを許したくない場合も考えられる。このような場合はログイン情報管

理オブジェクト114へのSID検証依頼処理(ステップ403)で、ログイン情報管理オブジェクト114にUIDも渡すようにし、ログイン情報管理オブジェクト114のセッション管理テーブル検索処理(ステップ404)でUIDの検索も行うことで実現できるユーザ認証オブジェクト112は返された検証結果を判定する(ステップ405)。結果が未登録の場合、認証処理(ステップ406)を行い、その結果を検証する(ステップ407)。認証が成功した場合はSID、UIDおよび認証時に得られるユーザ属性をログイン情報管理オブジェクト114に対し登録依頼する(ステップ408)。ログイン情報管理オブジェクト114は渡されたSID、UIDおよびユーザ属性をセッション管理テーブル201に登録する(ステップ409)。ユーザ認証オブジェクト112はSID、UIDおよびユーザ属性の登録処理依頼(ステップ408)後、正常終了コードをCGIプログラム109に返し処理を終了する。

【0017】図5はCGIプログラム109においてユーザ認証オブジェクト112からステップ405、407でエラーで返された場合およびステップ408後に正常終了コードが返された場合の後の処理の流れ図である。CGIプログラム109はユーザ認証オブジェクトへ112のログイン依頼処理(ステップ402)後、ユーザ認証オブジェクト112から返されたコードを判定する(ステップ501)。判定結果が正常である場合はアプリケーション画面をHTMLとして生成(ステップ502)し、またステップ501での判定結果がエラーである場合はログイン失敗画面をHTMLとして生成し(ステップ502)、Webブラウザに返す。Webブラウザは渡されたHTMLを表示する(ステップ504)。表示内容はCGIプログラムのログイン依頼処理(ステップ402)の結果によりアプリケーション実行画面か、「すでにログインしています。」などのログイン失敗画面となる。

【0018】図6はWebブラウザ102からアプリケーション実行操作を行ったときの流れ図である。これまで説明したログインが成功しWebブラウザ102上にアプリケーション実行画面が表示され、ユーザが実行操作を行う(ステップ601)。Webブラウザ12はSIDと必要であればアプリケーションのパラメタをCGIプログラムへ渡す。CGIプログラムはSIDとパラメタを指定し業務サーバオブジェクト116を実行する(ステップ602)。業務サーバオブジェクト116が実行されるとログイン情報管理オブジェクト114に渡されたSIDの検証依頼(ステップ603)を行う。ロ

グイン情報管理オブジェクト114は渡されたSIDがセッション管理テーブル201に存在するかを検索する(ステップ604)。見つかった場合は認証済みとなり、見つからない場合はログインされていないということになる。この結果を業務サーバオブジェクト116に返す。業務サーバオブジェクト116はログイン情報管理オブジェクト114より返された結果を判定する(ステップ605)。認証済みであれば業務処理を行い(ステップ606)その結果をCGIプログラム109に返す。ステップ605の判定結果がログインされていなければエラーコードをCGIプログラム109に返す。CGIプログラム109は業務サーバオブジェクト116から返された結果に対応した画面をHTMLとして生成し(ステップ607)、Webブラウザ102に返す。Webブラウザ102はCGIプログラム109が生成したHTMLを表示する(ステップ608)。

【0019】

【発明の効果】以上述べたように本発明によれば、ユーザ認証が必要な業務サーバオブジェクト116が分散オブジェクト基盤110を利用するネットワークに分散しており、クライアントからHTTPのような接続状態を管理しない通信プロトコルを使って業務サーバオブジェクト116を利用するクライアント・サーバシステムにおいて、認証済みのセッションの識別子と対応するユーザ情報とそのユーザ属性を一元管理することによって、シングルサインオンを実現できる。

【図面の簡単な説明】

【図1】システム全体構成図。

【図2】セッション管理テーブル。

【図3】認証処理フロー1。

【図4】認証処理フロー2。

【図5】認証処理フロー3。

【図6】認証処理フロー4。

【符号の説明】

101、103、105…クライアント計算機

102、104、106…Webブラウザ

107…WWW環境

108…Webサーバ計算機

109…CGIプログラム

110…分散オブジェクト基盤

113、115…オブジェクトサーバ計算機

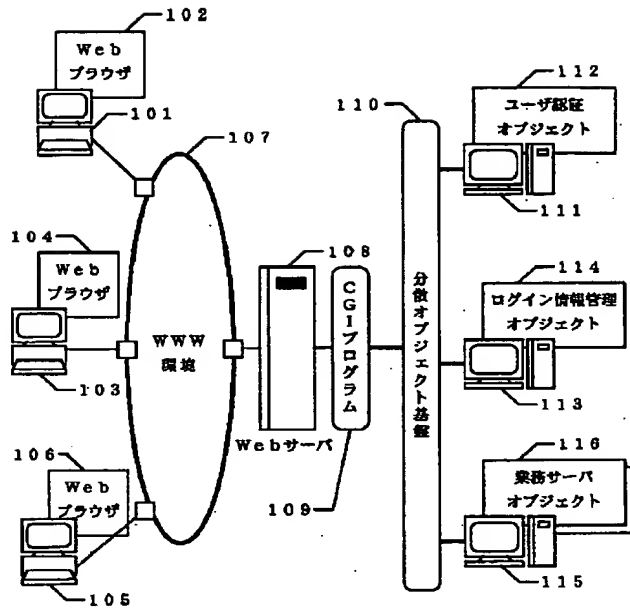
112…ユーザ認証オブジェクト

114…ログイン情報管理オブジェクト

116…業務サーバオブジェクト

【図1】

図1



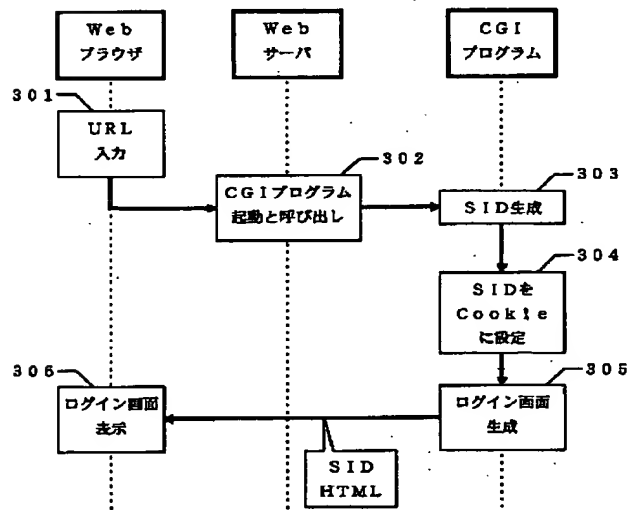
【図2】

図2

| SID | UID | ユーザ属性 |
|-------|-----|-------|
| 00001 | AAA | |
| 00002 | BBB | |
| 00003 | CCC | |
| 00004 | DDD | |
| ... | ... | ... |
| 00100 | XXX | |

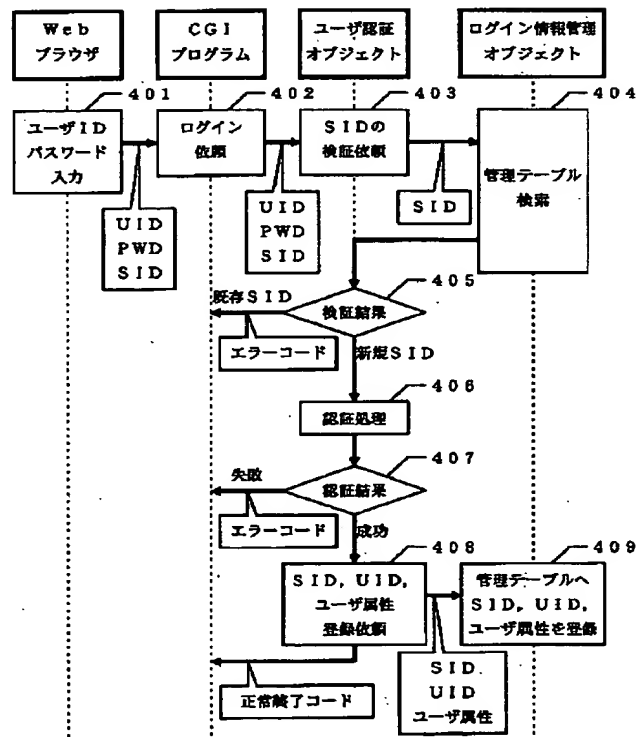
【図3】

図3

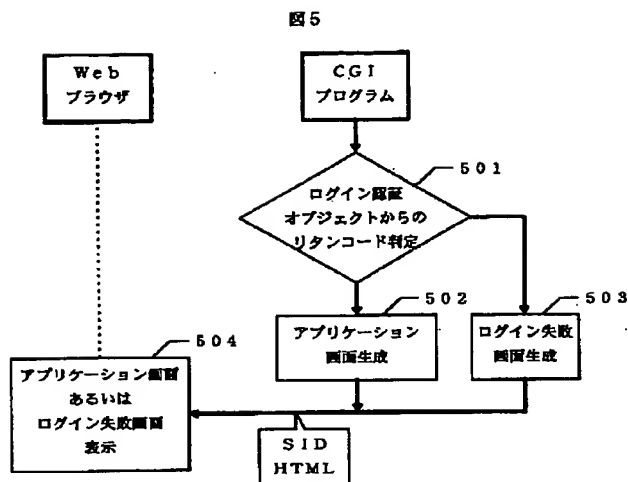


【図4】

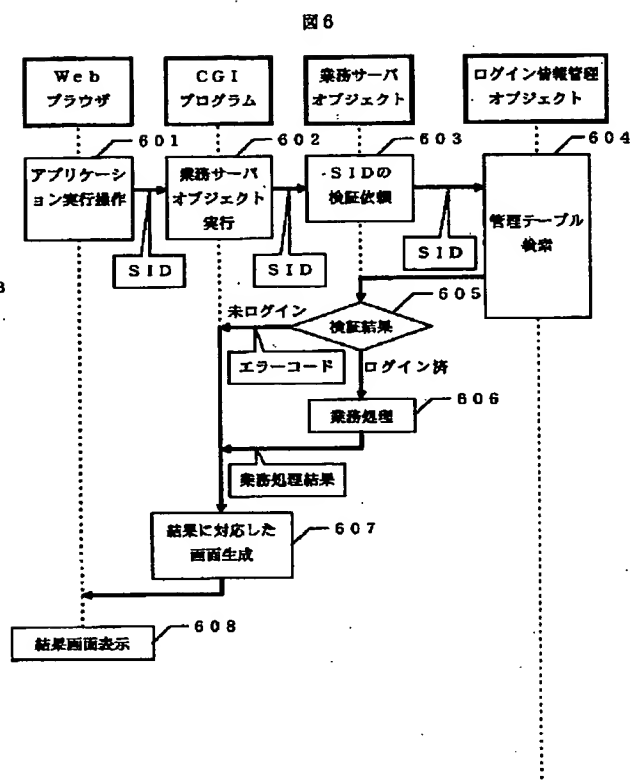
図4



【図5】



【図6】



フロントページの続き

(72)発明者 内田 稔
 神奈川県横浜市戸塚区戸塚町5030番地 株
 式会社日立製作所ソフトウェア事業部内
 (72)発明者 小瀧 伯泰
 神奈川県横浜市戸塚区戸塚町5030番地 株
 式会社日立製作所ソフトウェア事業部内

(72)発明者 内田 貴子
 神奈川県横浜市戸塚区戸塚町5030番地 株
 式会社日立製作所ソフトウェア事業部内
 Fターム(参考) 5B085 AC03 AE01 AE06 AE23 BC01
 BG07
 5J104 AA07 KA01 MA01 NA05 NA27
 PA09